

## REMARKS

Applicant respectfully requests reconsideration of this application. Claims 1-5, 7, 8, 10-12, 14-17, 19-21, 23-28, and 30-39 are pending. Claims 1, 3, 4, 17, 31, 32, 36, and 37 have been amended. Claims 38 and 39 have been cancelled. No claims have been added.

Therefore, claims 1-5, 7, 8, 10-12, 14-17, 19-21, 23-28, and 30-37 are now presented for examination.

### Claim Rejection under 35 U.S.C. §102

#### Jari et al.

The Examiner rejected claims 1, 5, 14, 17, 20, 28, 31, and 33 under 35 U.S.C. 102(b) as being anticipated by U.S Patent Publication 2001/0020275 of Jari, et al. (hereinafter referred to as "*Jari*").

It is submitted that *Jari* does not contain the elements of the claims.

Claim 1 reads as follows:

1. A method comprising:  
establishing secured communication between a client device and a server device, wherein communication is secured using, at least in part, a plurality of synchronized security sequence values for authentication of secure communications;  
storing a security sequence value from the plurality of synchronized security sequence values as a first resynchronization value;  
detecting at least one event desynchronizing said secured communication;  
requesting resynchronization of security sequence values, requesting resynchronization comprising sending at least a representation of said first resynchronization value from said client device to said server device;

receiving a second resynchronization value in a response to the first resynchronization value; and  
reestablishing secured communication using the first resynchronization value and the second resynchronization value.

It is submitted that *Jari* does not contain the elements of the claims. It is submitted that *Jari* does not describe a plurality of synchronized security sequence values, or the detection of an event desynchronizing the secured communications. Even if it is assumed for the sake of argument that other provisions are taught or suggested by *Jari*, *Jari* does not provide for “receiving a second resynchronization value in a response to the first resynchronization value” or for “reestablishing secured communication using the first resynchronization value and the second resynchronization value”.

*Jari* describes a communication node and a method of recovering from a temporary failure of the node. The process described by *Jari* is shown, for example, in Figure 2 and 3. As shown, upon a change in the security association database, there is an interrupt 12, followed by the SAD being provided to the controller 13, encrypted 14, and stored on disk 15. Upon a restoration of power 20 following a power loss, the most recent SAD is retrieved from disk and decrypted 23. Any expired security associations are deleted 24, and the SAD is written to CPU memory.

It is submitted that no sequence of synchronized security values is shown by *Jari*. What *Jari* shows is a plurality of security associations. Further, there is a sequence involved, each security association having a “header sequence number”. While the security values may have a sequence and have certain “lifetime information”, such values are not synchronized to anything. Similarly, the loss of power results in the loss of the

current SAD, but this is not an event desynchronizing the secured communications. It is rather simply the loss of data that needs to be retrieved.

However, even if other elements are assumed for the sake of argument to exist, then it is submitted that *Jari* does not provide for “receiving a second resynchronization value in a response to the first resynchronization value” or “reestablishing secured communication using the first resynchronization value and the second resynchronization value”. If *Jari* provides for transmission of a first resynchronization value (which is not the case), then there is no second resynchronization value. *Jari* does not teach or suggest any such operation, instead providing that secure communications can be restored using the SAD that is retrieved from memory. It thus follows that *Jari* does not provide for the reestablishment of secured communications using the first resynchronization value and the second resynchronization value.

It is submitted that the above arguments also apply to independent claims 5, 14, 17, 20, 28, 31, and 33, and thus such claims are also allowable.

In addition, it is submitted that an affidavit may be produced in order to swear behind the cited reference. It is submitted herein that such affidavit is not necessary because it has been shown herein that the reference is not relevant to the claims, as amended. However, the Applicant reserves the right to provide such affidavit if the Examiner maintains a rejection on the basis of *Jari*.

### **Claim Rejection under 35 U.S.C. §102**

#### **Gambino**

The Examiner rejected claims 1-4, 31-32, 36-37, and 39 under 35 U.S.C. 102(b) as being anticipated by U.S. Patent 6,339,796 of Gambino (“*Gambino*”).

It is again submitted that *Gambino* involves different technical issues and is not relevant to the claims.

Claim 1 provides for “establishing secured communications”, with communications being secured using, at least in part “a plurality of synchronized security sequence values for authentication of secure communications.” The other independent claims contain related elements regarding secure communications. The nature of secure communications regards different issues than simply synchronizing messages in the sense of ordering. The order of messages can be apparent, and the messages themselves can be accessed to obtain information regarding synchronization. Synchronized security sequence values involve different issues. The issue involves the synchronization of the security sequence values. If the proper key is not available for secured data, the data cannot be accessed. This is a very different issue than the question of data that is out of sequence because of component failure or similar issues.

In contrast, *Gambino* is not concerned with security sequence values or the authentication of secure communications. *Gambino* instead concerns re-synchronizing message traffic in a communications network following a network communications failure. As described in *Gambino*, a system transfers traffic between a first data processing system and a second data processing system, with each message in the message traffic including a SYNC number and byte sequence number (BSN). (*Gambino*, e.g., col. 2, lines 16-23) The BSN indicates a sequence of messages, with the message recipient testing to determine whether a message has the next expected, with older numbers being discarded. (*Gambino*, col. 2, lines 23-26) Further, a message transport header (THDR) contains a SYNC number to indicate new versions of control

information, with the recipient processing the control information if the SYNC number is equal to or higher the previous SYNC number and discarding the control information otherwise. (*Gambino*, col. 4, lines 59-67).

Thus, it is respectfully submitted that *Gambino* deals with a different solution to a different problem. *Gambino* is discussing a system to resynchronize and restart a network after a component failure through use of stored SYNC and BSN data, not with synchronized security values. *Gambino* thus is concerned with the ordering of data, not with the ordering of security sequences required to access such data. In *Gambino* there is no discussion of this type of security issues, or this type of synchronization. While *Gambino* discusses synchronization, it is discussing a different type of synchronization. In essence, *Gambino* discusses a way to figure out the status of a network when there is a component failure so that it can be quickly restored. This does not involve the same issues as are faced with sequences of security values that are needed to access data.

It is submitted that the arguments presented above also apply to independent claim 31 and thus such claim is also allowable. The remaining claims are dependent claims and allowable as being dependent on the allowable base claims.

### **Claim Rejection under 35 U.S.C. §103**

#### **Gambino in view of Johnson**

The Examiner rejected claims 5, 7-8, 10-12, 14-17, 19-21, 23-28, 30, 33-35, and 38 under 35 U.S.C. 103(a) as being unpatentable over *Gambino* in view of U.S Patent No. 6,247,059 of Johnson ("*Johnson*").

It is respectfully submitted that the discussion above regarding *Johnson* does not contain the elements missing from *Gambino*, or as missing from *Jari*. For this reason, the references, alone or in combination, do not teach or suggest the elements of the claims.

*Johnson* generally involves transmission of multicast messages to members of a computing system. Again, re-synchronization is an issue, but not in reference to security values. For example, *Johnson* claims a method that involves receiving at least one of a sequence of multicast messages, comparing a “time of life” indicated by a marker to a time of life of a prior message, and sending a resynchronization message to a sender node if the times of life “do not compare”. (*Johnson*, claim 1)

As with *Gambino*, a type of resynchronization is involved in *Johnson* that is different than the claims and does not involve synchronized security values for the authentication of secure communications.

For at least the above reasons, *Gambino* and *Johnson*, alone or in combination, do not teach or suggest the elements of the claims.

### **Conclusion**

Applicant respectfully submits that the rejections have been overcome by the amendment and remark, and that the claims as amended are now in condition for allowance. Accordingly, Applicant respectfully requests the rejections be withdrawn and the claims as amended be allowed.



### **Invitation for a Telephone Interview**

The Examiner is requested to call the undersigned at (503) 439-8778 if there remains any issue with allowance of the case.

### **Request for an Extension of Time**

The Applicant respectfully petitions for an extension of time to respond to the outstanding Office Action pursuant to 37 C.F.R. § 1.136(a) should one be needed. Please charge any fee for such extension to our Deposit Account No. 02-2666.

### **Charge our Deposit Account**

Please charge any shortage to our Deposit Account No. 02-2666.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP

Date: July 11, 2006

/Mark C. Van Ness/

Mark C. Van Ness, Reg. No. 39,865

12400 Wilshire Boulevard  
7<sup>th</sup> Floor  
Los Angeles, California 90025-1026  
(503) 439-8778